CLAIMS

What is claimed is:

1. A method, comprising:

connecting a device to a network;

determining a unique identifier based on the network;

obtaining network configuration settings that are associated with the unique network identifier;

intercepting network traffic originating from an application located on the device; and

rerouting the intercepted network traffic to a final correct location using the obtained network configuration settings.

2. The method of claim 1 wherein the unique network identifier is comprised of one or more items from a group consisting of an Internet protocol address, a subnet mask, a domain name server address, a domain name server suffix, a default gateway, and a dynamic host configuration protocol.

3. The method of claim 1 wherein connecting a device to a network and determining a unique identifier based on the network further comprises:

monitoring the connection between the device and the network;

detecting a change in network connectivity; and

determining the unique network identifier after a change in network connectivity.

4. The method of claim 1 wherein obtaining network configuration settings that are associated with the unique network identifier further comprises:

storing a list of information relating to one or more networks including at least a unique network identifier for each network and an associated set of network configuration settings for each network; and

looking up the unique network identifier in the stored list and obtaining the network configuration settings associated with that unique network identifier in the stored list.

5. The method of claim 1 wherein intercepting network traffic originating from an application located on the device further comprises:

monitoring the network connection between the device and the network for outbound traffic from the device; and

preventing outbound traffic from exiting the device.

6. The method of claim 5 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

emulating a network interface card with the network service; and

directing application network traffic to the emulated network interface card.

7. The method of claim 5 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

assigning the network service a unique network port number for each network-enabled application; and

directing application network traffic to the unique network port number associated with the application.

8. The method of claim 5 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

assigning the network service a unique network port number for each network protocol; and

directing application network traffic to the unique network port number associated with the applicable network protocol.

9. The method of claim 5 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

emulating a SOCKS server with the network service; and

directing application network traffic to the emulated SOCKS server.

10. The method of claim 4 wherein rerouting the intercepted network traffic to a final correct location using the obtained network configuration settings further comprises:

determining the correct network protocol and final destination address by analyzing the network traffic originating from the application;

routing the traffic to the proper destination address by utilizing the determined network protocol, the final destination address, and the obtained network configuration settings.

11. A machine readable medium having embodied thereon instructions, which when executed by a machine, comprises:

connecting a device to a network;

determining a unique identifier based on the network;

obtaining network configuration settings that are associated with the unique network identifier;

intercepting network traffic originating from an application located on the device; and

rerouting the intercepted network traffic to a final correct location using the obtained network configuration settings.

12. The machine readable medium of claim 11 wherein connecting a device to a network and determining a unique identifier based on the network further comprises:

monitoring the connection between the device and the network;

detecting a change in network connectivity; and

determining the unique network identifier after a change in network connectivity.

13. The machine readable medium of claim 11 wherein obtaining network configuration settings that are associated with the unique network identifier further comprises:

storing a list of information relating to one or more networks including at least a unique network identifier for each network and an associated set of network configuration settings for each network; and

looking up the unique network identifier in the stored list and obtaining the network configuration settings associated with that unique network identifier in the stored list.

14. The machine readable medium of claim 11 wherein intercepting network traffic originating from an application located on the device further comprises:

monitoring the network connection between the device and the network for outbound traffic from the device; and

preventing outbound traffic from exiting the device.

15. The machine readable medium of claim 14 wherein rerouting the intercepted network traffic to a final correct location using the obtained network configuration settings further comprises:

determining the correct network protocol and final destination address by analyzing the network traffic originating from the application;

routing the traffic to the proper destination address by utilizing the determined network protocol, the final destination address, and the obtained network configuration settings.

16. A system, comprising:

a bus;

a processor coupled to the bus;

a network interface coupled to the bus; and

memory coupled to the processor, the memory adapted for storing instructions, which upon execution by the processor connect a device to a network, determine a unique identifier based on the network, obtain network configuration settings that are associated with the unique network identifier, intercept network traffic originating from an application located on the device, and reroute the intercepted network traffic to a final correct location using the obtained network configuration settings.

17. The system of claim 16 wherein the unique network identifier is comprised of one or more items from a group consisting of an Internet protocol address, a subnet mask, a domain name server address, a domain name server suffix, a default gateway, and a dynamic host configuration protocol.

18. The system of claim 16 wherein connecting a device to a network and determining a unique identifier based on the network further comprises:

monitoring the connection between the device and the network;

detecting a change in network connectivity; and

determining the unique network identifier after a change in network connectivity.

19. The system of claim 16 wherein obtaining network configuration settings that are associated with the unique network identifier further comprises:

storing a list of information relating to one or more networks including at least a unique network identifier for each network and an associated set of network configuration settings for each network; and

looking up the unique network identifier in the stored list and obtaining the network configuration settings associated with that unique network identifier in the stored list.

20. The system of claim 16 wherein intercepting network traffic originating from an application located on the device further comprises:

monitoring the network connection between the device and the network for outbound traffic from the device; and

preventing outbound traffic from exiting the device.

21. The system of claim 20 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

emulating a network interface card with the network service; and

directing application network traffic to the emulated network interface card.

22. The system of claim 20 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

assigning the network service a unique network port number for each network-enabled application; and

directing application network traffic to the unique network port number associated with the application.

23. The system of claim 20 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

assigning the network service a unique network port number for each network protocol; and

directing application network traffic to the unique network port number associated with the applicable network protocol.

24. The system of claim 20 wherein intercepting network traffic originating from an application located on the device further comprises:

implementing a network service on the device;

emulating a SOCKS server with the network service; and

directing application network traffic to the emulated SOCKS server.

25. The system of claim 19 wherein rerouting the intercepted network traffic to a final correct location using the obtained network configuration settings further comprises:

determining the correct network protocol and final destination address by analyzing the network traffic originating from the application;

routing the traffic to the proper destination address by utilizing the determined network protocol, the final destination address, and the obtained network configuration settings.